Available online at www.sciencedirect.com

SCIENCE DIRECT

ELSEVIER

European Journal of Combinatorics 28 (2007) 653–664

European Journal of Combinatorics

www.elsevier.com/locate/ejc

A generalized quadrangle with an automorphism group acting regularly on the points

Satoshi Yoshiara

Department of Mathematics, Tokyo Woman's Christian University, Zempukuji 2-6-1, Suginami-ku, Tokyo 167-8585, Japan

Available online 29 August 2005

Abstract

We develop several fundamental lemmas on a generalized quadrangle with an automorphism group acting regularly on its set of points. This can be thought of as an improvement of arguments originated in D. Ghinelli [Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1, Geom. Dedicata 41 (1992) 165–174], not depending on representation theoretic results in U. Ott [Some remarks on representation theory in finite geometries, in: Geometries and Groups, in: Lecture Notes in Math. vol. 893, 1981, pp. 68–110]. Based on them, we show that there is no generalized quadrangle of order (t^2, t) $(t \geq 2)$ with such an automorphism group.

1. Introduction

In this introduction, we tentatively call a generalized quadrangle *regular* if it admits an automorphism group acting regularly on its set of points. Such an automorphism group is also called *regular*. For example, if q is an odd (resp. even) prime power, then the generalized quadrangle of Ahrens and Szekeres $AS(q)$ [6, 3.1.5,3.2.6] (resp. of Tits $T_2^*(O)$ [6, 3.1.3,3.2.6]) of order $(q-1, q+1)$ admits a non-abelian (resp. abelian) regular automorphism group. Recently, De Winter and K. Thas [1] characterized regular generalized quadrangles with abelian regular groups as generalized quadrangles having

E-mail address: yoshiara@lab.twcu.ac.jp.

doi:10.1016/j.ejc.2004.11.004

'generalized linear representation' (in particular their orders are $(q-1, q+1)$ for some even prime power q).

The study of regular generalized quadrangles was initiated by D. Ghinelli [2], who considered the structure of regular automorphism groups in general, not only in the abelian case. Her main idea is that if a regular generalized quadrangle has order (s, s) then we can construct difference sets with correlations, whence we can exploit the results obtained by representation theoretic methods in [5]. However, the latter results are far from being elementary and can be applied only to generalized quadrangles of restricted order.

The author's interest in the present paper is in extending the results in [2]. It turns out that we can prove the fundamental results of [2] (including those which are only implicit in [2]), by much more elementary arguments. Specifically we impose no restriction on orders and we do not depend on [5] (see Section 2). Furthermore, we can show that the lemmas in Section 2 are powerful enough to derive restrictions on normal p-subgroups of regular automorphism groups stronger than those obtained in [2]. This turns out to be the case when a quadrangle is of order (t^2, t), (s, s), (s^2, s^3) or $(s+1, s-1)$.

For instance, using those fundamental lemmas and a classical result in the theory of finite groups, namely, a characterization of the Suzuki groups as simple $3'$-groups [4, Chapter II, Corollary 7.3], we obtain the following result.

Theorem 1. *There is no finite generalized quadrangle $\mathcal{Q} = (\mathcal{P}, \mathcal{L}; *)$ of order (t^2, t) which admits an automorphism group G acting regularly on $\mathcal{P}$.*

As for the other known orders except $(q-1, q+1)$, similar analyses yield restrictions on regular automorphism groups, some of which are unlikely to be satisfied. However, they are omitted in the present paper, as the results so far obtained by the author were just partial.

2. Basic results

2.1. Basic assumption and notation

Throughout this paper, we consider *a finite generalized quadrangle $\mathcal{Q} = (\mathcal{P}, \mathcal{L}; *)$ of order (s, t) with $s, t \geq 2$ for which a group G of automorphisms acts regularly on the set $\mathcal{P}$ of points.* In particular, from [6, 1.2.1] we have

$$|G| = |\mathcal{P}| = (s+1)(st+1).$$

For two distinct points P and Q (resp. lines l and m), we write $P \sim Q$ if they are collinear (resp. $l \sim m$ if they are *concurrent*, that is, l meets m in a point). We fix a point O, and let

$$\Delta := \{g \in G \mid O^g \sim O\} \cup \{1\}.$$

This subset already plays an important role in [2]. Note that $O^g \sim O$ iff $O \sim O^{g^{-1}}$. Thus $g \in \Delta$ iff $g^{-1} \in \Delta$.

For every line l through O, we set

$$\Delta(l) := \{g \in G \mid O^g \in l\} \cup \{1\}.$$

Clearly $\Delta \setminus \{1\}$ is the disjoint union of $\Delta(l) \setminus \{1\}$ with l ranging over the lines through O. We also use the symbol Δ^c to denote the set complementary to Δ in G.

For each nontrivial automorphism $g \in G$, the point-set is naturally divided into the following two parts, as g does not fix any point by our assumption:

$$\mathcal{P}_2(g) = \{P \in \mathcal{P} \mid P^g \sim P\}, \quad \mathcal{P}_3(g) = \{P \in \mathcal{P} \mid P^g \not\sim P\}.$$

On the other hand, the set of lines is the disjoint union of the following three subsets:

$$\mathcal{L}_1(g) = \{l \in \mathcal{L} \mid l^g = l\}, \quad \mathcal{L}_2(g) = \{l \in \mathcal{L} \mid l^g \sim l\},$$
$$\mathcal{L}_3(g) = \{l \in \mathcal{L} \mid l \neq l^g \not\sim l\}.$$

It is evident that $P \sim P^a$ iff $P^{a^{-1}} \sim P$ and $l \sim l^a$ iff $l^{a^{-1}} \sim l$ for a point P and a line l. Thus $\mathcal{P}_i(a) = \mathcal{P}_i(a^{-1})$ $(i = 2, 3)$ and $\mathcal{L}_i(a) = \mathcal{L}_i(a^{-1})$ $(i = 1, 2, 3)$ for every $1 \neq a \in G$.

For an element $a \in G$, we set

$$a^G := \{a^g = g^{-1}ag \mid g \in G\},$$

the conjugacy class of a under G.

2.2. Fundamental lemmas

We immediately have the following observations.

Lemma 2. (1) *If $a \in G$ is of order 2 or 3, we have $\mathcal{L}_2(a) = \emptyset$.*
(2) *If a nontrivial subgroup H of G stabilizes a line, then $|H|$ divides $s + 1$.*

Proof. (1) Suppose $l \in \mathcal{L}_2(a)$. If a is an involution then it fixes the point $P = l \cap l^a$, contrary to the regularity of G on $\mathcal{P}$. If it has order 3, then the lines l, l^a, l^{a^2} are pairwise concurrent, whence they pass through a unique point P, which is then fixed by a; again, a contradiction.
(2) The claim follows from the regularity of G on $\mathcal{P}$. $\square$

The following result is a fundamental tool for analyzing a generalized quadrangle $\mathcal{Q}$ with a regular automorphism group G on the points. It is just a corollary of [6, 1.9.1,1.9.2], which are obtained by using standard eigenvalue techniques and hold for every order (s, t). On the other hand, in [2] a similar formula (Eq. (8)) was obtained by relying on a result of Ott [5, 1.4], whose proof is less elementary. Furthermore, Ott's result is applicable only when Δ above defines a difference set in G, that is when $s = t$.

Lemma 3. *For a nontrivial automorphism $a \in G$, we have*

$$|\mathcal{P}_2(a)| = (s+1)|\mathcal{L}_1(a)| + |\mathcal{L}_2(a)| = |a^G \cap \Delta||C_G(a)| \tag{1}$$
$$= (s+1)(t+1) + (s+t)u_a \tag{2}$$

for some integer u_a. Furthermore, we have

$$|a^G \cap \Delta^c||C_G(a)| = t(s-1)(s+1) - (s+t)u_a. \tag{3}$$

Proof. As a fixes no point, it follows from [6, 1.9.1,1.9.2] that we have $|\mathcal{P}_2(a)| = (s+1)|\mathcal{L}_1(a)| + |\mathcal{L}_2(a)| = (s+1)(t+1) + (s+t)u_a$ for some integer u_a. For $x \in G$,

O^x lies in $\mathcal{P}_2(a)$ iff $O^x \sim O^{xa}$ (as $a \neq 1$) iff $O \sim O^{xax^{-1}}$, which is equivalent to $xax^{-1} \in a^G \cap \Delta$. As $xax^{-1} = yay^{-1}$ for $x, y \in G$ iff $x^{-1}y \in C_G(a)$, we see that $|\mathcal{P}_2(a)| = |a^G \cap \Delta||C_G(a)|$. Thus we have verified all equalities except the last one.

As $|a^G \cap \Delta^c| = |a^G| - |a^G \cap \Delta|$ and $|a^G||C_G(a)| = |G| = (s+1)(st+1)$, the last equality follows from the former. □

The next two observations implicitly appeared in the proofs of [2, Lemma 3.3,Lemma 3.6]. Here we denote by G_l the stabilizer of a line l in G.

Lemma 4. *Let H be a nontrivial subgroup of G which is entirely contained in the set Δ (defined in 2.1). Then there is a unique line l through O such that $H \leq G_l$.*

Proof. Choose a nontrivial element a of H. Then $O \sim O^a$ as $a \in \Delta \setminus \{1\}$. Let l be the line through O and O^a. For every $x \in H$, we have $xa^{-1} \in H \subset \Delta$, and $O \sim O^{xa^{-1}}$. Then $O^a \sim O^x$, as the automorphism x preserves the collinearity. On the other hand, $O \sim O^x$, as $x \in H \subseteq \Delta$. Hence O^x is collinear with two distinct points O and O^a on the line l, and hence $O^x \in l$. So far, $H \leq \Delta(l)$. It is now clear that $H \leq G(l)$.

If l and m are distinct lines through O such that $H \leq G_l \cap G_m$, then H fixes the point O of intersection of l with m, and so $H = 1$ by the regularity of G. This contradiction shows the uniqueness of l. □

Lemma 5. *Let X be a subset of $G \setminus \{1\}$ which consists of mutually commuting elements. For every line l through the point O we have either*

$$|X \cap \Delta(l)| \leq 1 \qquad \textit{or} \qquad \langle X \cap \Delta(l)\rangle \leq G_l$$

Proof. Assume that $|X \cap \Delta(l)| \geq 2$ for some line l through O. Let a and b be any distinct elements of $X \cap \Delta(l)$. Then O^a and O^b are two distinct points of l. In particular, $O \sim O^a$ and $O \sim O^b$. As the action of G preserves collinearity, using the commutativity of X we have

$$O^b \sim (O^a)^b = O^{ab} = O^{ba} = (O^b)^a \sim O^a.$$

Thus $O^{ab} \sim O^a, O^b \in l$. Hence $O^{ab} \in l$. It follows that $\langle X \cap \Delta(l)\rangle \subseteq \Delta(l)$. Hence $\langle X \cap \Delta(l)\rangle \leq G_l$ (compare Lemma 4). □

2.3. Restrictions on normal subgroups

Lemma 6. *Let a be any nontrivial element of G, and let $d = (s, t)$ be the greatest common divisor of s and t. Then the following hold.*

(1) *If $d > 1$, then $a^G \cap \Delta \neq \emptyset$.*
(2) *$|a^G \cap \Delta^c|$ is a multiple of d (possibly equal to 0).*

Proof. (1) Suppose $a^G \cap \Delta = \emptyset$. Then it follows from Eq. (1) in Lemma 3 that

$$0 = |a^G \cap \Delta||C_G(a)| = (s+1)(t+1) + (s+t)u_a$$

for some integer u_a. Thus $s+t$ divides $st+1$. In particular, $1 < d = (s,t)$ divides $st+1$, but $st+1 \equiv 1 \pmod{d}$.

(2) As d divides both t and $s+t$, it follows from Eq. (3) in Lemma 3 that $|a^G \cap \Delta^c||C_G(a)|$ is a multiple of d. On the other hand, $|G| = (s+1)(st+1) \equiv 1 \pmod{d}$. Thus d is prime to $|G|$, and hence to $|C_G(a)|$. Then d divides $|a^G \cap \Delta^c|$. □

Lemma 7. *Assume that $d = (s,t) > 1$ and let $p = 2$ or 3. Then the following conditions are equivalent.*

(a) *$|G|$ is divisible by p.*
(b) *There is an element of order p of G which fixes a line l through O.*
(c) *$s+1$ is divisible by p.*

Proof. Assume that (a) holds, and let a be an element of order p of G. By Lemma 2(1) and Lemma 3, we have $(s+1)|\mathcal{L}_1(a)| = |a^G \cap \Delta||C_G(a)|$. As $|a^G \cap \Delta| \neq 0$ by Lemma 6(1), we see $\mathcal{L}_1(a) \neq \emptyset$. Thus for a line $l \in \mathcal{L}_1(a)$ we have $a \in G_l$, and (b) holds.

If (b) holds, then (c) follows from Lemma 2(2). Trivially (c) implies (a). □

Lemma 7 shows that G is a $3'$-group (a finite group of order coprime to 3), if $s+1$ is not a multiple of 3 (e.g. when s is a square). For a $3'$-group, its sections (quotient groups of subgroups) can be determined from classical results [4,3] in the theory of finite groups (independent of the classification of finite simple groups). For the proof of Theorem 1 in the next section, we only need claim (1) below. However, claim (2) is added as a supplement.

Theorem 8. *Assume that $d = (s,t) > 1$ and $s+1$ is prime to 3. Then the following hold.*

(1) *If G has a non-abelian minimal normal subgroup N, then $N = S_1 \times S_2 \times \cdots \times S_m$ with each S_i $(i = 1, \ldots, m)$ isomorphic to the Suzuki group ${}^2B_2(q) = Sz(q)$ for some $q = 2^{2e+1} \geq 8$, not depending on i.*
(2) *If $|G|$ is even, then there is a strongly closed abelian 2-subgroup A of G containing $\Omega_1(Z(P))$ for a Sylow 2-subgroup P of G. Hence the normal closure $K := \langle A^g \mid g \in G \rangle$ in G has the following structure, allowing $n = 0$:*

$$K/O(K) \cong S_1 \times \cdots S_n \times D,$$

where $O(K)$ denotes the largest normal subgroup of K of odd order, S_i is isomorphic to the Suzuki group $Sz(q_i)$ for some $q_i = 2^{2e_i+1}$, depending on i $(i = 1, \ldots, n)$ and D is an abelian 2-group (possibly trivial).

Proof. It follows from Lemma 7 that G is a $3'$-group. It is known that a nonabelian finite simple $3'$-group is isomorphic to $Sz(q)$ for some q [4, Chapter II,Corollary 7.3]. As a nonabelian minimal normal subgroup of G is isomorphic to a direct product of mutually isomorphic nonabelian simple groups, claim (1) follows.

Furthermore, G is S_4-free, that is, no section of G is isomorphic to the symmetric group S_4 of degree 4. From the above characterization of the Suzuki groups, every composition factor of any section of G is either abelian or one of the Suzuki groups. Hence the assumptions of [4, Chapter II,Proposition 6.1] are satisfied. Thus, if $|G|$ is even, denoting by $J_e(P)$ a Sylow 2-subgroup P of G, the subgroup generated by all elementary abelian subgroups of P of maximum possible order, then the subgroup A generated by the conjugates of $\Omega_1 Z(P)$ under $N_G(J_e(P))$ is a strongly closed elementary abelian

2-subgroup of G (that is, $A^g \cap P \leq A$ for every $g \in G$). The structure of the normal closure K of A in G is then determined by Goldschmidt [3] as stated in claim (2) above. $\square$

Lemma 9. *Assume that there is a nontrivial normal subgroup N of G, which satisfies one of the following conditions:*

(i) *N is entirely contained in Δ.*
(ii) *N is a p-subgroup for a prime p coprime with $|\mathcal{L}|$.*

Then the following hold.

(1) *There is a line l through O such that $|G_l| = s+1$ and $l^G := \{l^g \mid g \in G\}$ forms a spread in $\mathcal{Q}$ (that is, l^G is a set of $st+1$ mutually nonconcurrent lines, or equivalently, every point is contained in just a single member of l^G). In particular, $s \leq t^2 - t$.*
(2) *$|N|$ divides the greatest common divisor $(s+1, t^2-t)$.*

Proof. Let N be a nontrivial normal subgroup of G satisfying the assumption of the claim. If N is a p-subgroup for a prime p with $(p, |\mathcal{L}|) = 1$, then N fixes at least one line l. As N is normal in G, replacing l by its suitable conjugate under G, we may assume that l contains the fixed point O. If $N \subseteq \Delta$, then it follows from Lemma 4 that $N \leq G_l$ for some line l through O. Thus in either case, we have $N \leq G_l$ for some line l through O.

Then $N = N^g \leq G_l^g = G_{l^g}$ for every $g \in G$, as N is normal in G. Since N is nontrivial, the regularity of G implies that two distinct lines l^g and l^h $(g, h \in G)$ are not concurrent. Thus $\mathcal{S} := \{l^g \mid g \in G\}$ forms a set of mutually nonconcurrent lines, and hence $|G : G_l| = |\mathcal{S}| \leq st+1$. On the other hand, we have $|G_l| \leq s+1$ by Lemma 2(2), and hence $|G : G_l| \geq st+1$. Thus $|\mathcal{S}| = |G : G_l| = st+1$, and $\mathcal{S}$ is a spread of $\mathcal{Q}$. Then it follows from the dual statement of [6, 1.8.3] that $s \leq t^2 - t$. Claim (1) is verified.

Furthermore, we see that N acts semiregularly on $\mathcal{L} \setminus \mathcal{S}$ as follows. For each line $m \in \mathcal{L} \setminus \mathcal{S}$, there is $g \in G$ such that m^g contains O. Then $l \cap m^g = O$, and hence $G_l \cap G_{m^g} = 1$ by the regularity of G. Hence $N \cap G_{m^g} \leq G_l \cap G_{m^g} = 1$, and $1 = N_{m^g} = (N_m)^g$ by the normality of N. Then $N_m = 1$ for every line $m \in \mathcal{L} \setminus \mathcal{S}$. Thus N acts semiregularly on $\mathcal{L} \setminus \mathcal{S}$, and $|N|$ divides $|\mathcal{L} \setminus \mathcal{S}| = (t+1)(st+1) - (st+1) = t(st+1)$. On the other hand, as $N \leq G_l$, $|N|$ divides $s+1 = |G_l|$. Hence $|N|$ divides the common divisor $(t(st+1), s+1) = (t(-t+1), s+1)$, and claim (2) follows. $\square$

The following lemma furthermore restricts the structure of N when condition (i) in Lemma 9 is satisfied.

Lemma 10. *Assume that $d = (s,t) > 1$ and that the conjugacy class a^G of a nontrivial element $a \in G$ is entirely contained in Δ. Then the following hold for every $i = 1, \dots, n-1$, where n denotes the order of a.*

(1) *$\mathcal{L}_1(a^i) = \mathcal{L}_1(a)$, $\mathcal{L}_2(a^i) = \emptyset$, $\mathcal{P} = \mathcal{P}_2(a^i)$, and $(a^i)^G \subseteq \Delta$.*
(2) *The set $\mathcal{L}_1(a)$ of lines fixed by a forms a spread. In particular, $s \leq t^2 - t$.*
(3) *The order n of a divides $s+1$.*

Proof. The assumption $a^G \subseteq \Delta$ holds iff $|\mathcal{P}_2(a)| = |a^G \cap \Delta||C_G(a)| = |a^G||C_G(a)| = |G| = |\mathcal{P}|$ by Eq. (1) in Lemma 3, which is equivalent to $\mathcal{P} = \mathcal{P}_2(a)$.

We first note that $\mathcal{L}_2(a) = \emptyset$. Suppose not. Then there exists a line l intersecting with l^a at a point P, say. Let Q be a point on the line l distinct from P and $P^{a^{-1}}$. (As $2 \leq d \leq s$, such a point exists.) As $Q \in \mathcal{P} = \mathcal{P}_2(a)$, we have $Q^a \sim Q$. We also have $Q^a \sim P$, as those points lie on the line l^a. Thus Q^a is collinear with two distinct points P and Q on the line l, and hence Q^a lies on l. But then $\{Q^a\} = l \cap l^a = \{Q\}$, which contradicts $a \neq 1$.

Hence we have $|\mathcal{P}_2(a)| = (s+1)|\mathcal{L}_1(a)|$ by Eq. (1) of Lemma 3. As $(s+1)(st+1) = |\mathcal{P}| = |\mathcal{P}_2(a)|$ by the remark at the first paragraph, we have $|\mathcal{L}_1(a)| = st + 1$. By the regularity of G, no two distinct lines of $\mathcal{L}_1(a)$ (as well as $\mathcal{L}_1(a^i)$ for all $i = 1, \ldots, n-1$) are concurrent, and so $|\mathcal{L}_1(a^i)| \leq st + 1$ for $i = 1, \ldots, n-1$. Thus $\mathcal{L}_1(a)$ is a spread. As $\mathcal{L}_1(a) \subseteq \mathcal{L}_1(a^i)$, we have that $\mathcal{L}_1(a) = \mathcal{L}_1(a^i)$ is a spread for every $i = 1, \ldots, n-1$.

Then it follows from the relation $|\mathcal{P}_2(a^i)| = (s+1)|\mathcal{L}_1(a^i)| + |\mathcal{L}_2(a^i)| \leq |\mathcal{P}| = |G|$ that $\mathcal{L}_2(a^i) = \emptyset$, $\mathcal{P}_2(a^i) = \mathcal{P}$, and hence $(a^i)^G \subseteq \Delta$ for every $i = 1, \ldots, n$. We have established claims (1) and (2).

(3) As $a \in \Delta$, the point O is collinear with O^a. Let l be the line through those points. If $a^2 = 1$, then a interchanges O and O^a, and hence $a \in G_l$. If $a^2 \neq 1$, then $O^a \sim O^{a^2} \sim O$, as $a^2 \in \Delta$. Then $O^{a^2} \in l$. Thus $l^a = l$, namely $a \in G_l$. Thus in either case, a acts on the set of $s+1$ points on the line l, and claim (3) follows from the regularity of G on $\mathcal{P}$. □

3. The case when $(s, t) = (t^2, t)$

In this section, we will prove Theorem 1 as an application of the lemmas in the last section.

In the rest of this section, we assume that $\mathcal{Q} = (\mathcal{P}, \mathcal{L}; *)$ is a finite generalized quadrangle of order (t^2, t) with an automorphism group G acting regularly on $\mathcal{P}$. We also use the symbol x_p to denote the p-part of a natural number x, i.e., the power of a prime p such that x/x_p is coprime with p. The proof will be divided into several steps.

Step 1. We have the following.

(1) G is a $3'$-group.
(2) $|G| = (t+1)(t^2+1)(t^2-t+1)$, where $(t+1, t^2+1) = 1$ or 2 according to whether t is odd or even, and $(t+1, t^2-t+1) = (t^2+1, t^2-t+1) = 1$. Furthermore, $|G|_2 = 2(t+1)_2$ if t is odd and $|G|_2 = 1$ if t is even.
(3) If N is a nontrivial normal subgroup of G, then $|N| \geq t+2$. In particular, $O_p(G) = 1$ for every odd prime divisor p of $t+1$.
(4) $O_p(G) = 1$ for every odd prime divisor p of t^2+1.

Proof. (1) As $s = t^2$ is a square, $s+1$ is prime to 3. Thus the claim follows from Lemma 7.
(2) This is obtained just by arithmetic on the factors of $|G| = |\mathcal{P}| = (t^2+1)(t^3+1)$ with claim (1) above. Note that $(t+1, t^2-t+1) = 1$ or 3 in general, but we may apply (1) to eliminate the latter possibility.
(3) Suppose N is a nontrivial subgroup of G of order at most $t+1$. Then for every nontrivial element a of N, the size of the class a^G is at most t. In particular, $a^G \cap \Delta^c = \emptyset$, for otherwise $|a^G \cap \Delta^c|$ is a positive multiple of $d = (t^2, t) = t$ by Lemma 6(2) and so

$|a^G| = |a^G \cap \Delta| + |a^G \cap \Delta^c| \geq 1 + t$ by Lemma 6(1). Then $N \subseteq \Delta$. Thus there is a spread in $\mathcal{Q}$ by Lemma 9, as N satisfies condition (i) of Lemma 9. However, this implies $s = t^2 \leq t^2 - t$, which is a contradiction.

For an odd prime divisor p of $t+1$, we have $|G|_p = (t+1)_p$ from claim (2) above. Then the latter remark follows from the former.

(4) This also follows from Lemma 9, because the greatest common divisor of $t^2 + 1$ and $|\mathcal{L}| = (t+1)(t^3+1) = (t+1)^2(t^2-t+1)$ is $(t^2+1, t+1) = 1$ or 2 by claim (1), and so $N = O_p(G)$ for an odd prime divisor p of t^2+1 satisfies assumption (ii) of that lemma. $\square$

Step 2. We have $O_2(G) = 1$.

Proof. If t is even, then $|G| = (t+1)(t^2+1)(t^2-t+1)$ is odd, and the claim trivially holds. Thus we may assume that t is odd. Then $t^2+1 \equiv 2 \pmod 4$ and $|G|_2 = 2(t+1)_2$. Suppose $N := O_2(G) \neq 1$. From Step 1(3), we have $|N| \geq t+2$. As $|N|$ is a divisor of $|G|_2 = 2(t+1)_2$, this implies that $t+1$ is a power of 2 and $|N| = |G|_2 = 2(t+1)$. Thus N is a unique Sylow 2-subgroup of G. As every proper subgroup of N is of order at most $t+1$, it follows from Step 1(3) that N does not contain nontrivial normal subgroups of G. Thus the 2-subgroup N has no proper nontrivial characteristic subgroup, and hence N is elementary abelian.

Let a_i^G $(i = 1, \ldots, m)$ be all distinct conjugacy classes of G contained in $N - \{1\}$. We set $\alpha_i := |a_i^G \cap \Delta|$ and $\beta_i := |a_i^G \cap \Delta^c|/t$. Then each α_i is a positive integer by Lemma 6(1). By Lemma 6(2), each β_i is a nonnegative integer. If $\beta_i = 0$ for some i, then $a_i^G \subseteq \Delta$, and hence $s = t^2 \leq t^2 - t$ from Lemma 10. This contradiction shows that all β_i are positive. Now we have

$$|N| - 1 = 2t + 1 = \sum_{i=1}^{m} |a_i^G| = \sum_{i=1}^{m} \alpha_i + t\left(\sum_{i=1}^{m} \beta_i\right).$$

If $m \geq 2$, then $\sum_{i=1}^m \alpha_i \geq m \geq 2$ and $\sum_{i=1}^m \beta_i \geq 2$, and hence the right hand side of the above equation is at least $2 + 2t$, which is a contradiction. Thus $m = 1$ and $|a_1^G| = |G|/|C_G(a_1)| = 2t+1$. However, as N is abelian and so $N \leq C_G(a_1)$, this implies that $2t+1$ divides $|G|/|N| = ((t^2+1)/2)(t^2-t+1)$. Now we may verify that $(2t+1, (t^2+1)/2) = (2t+1, 5)$ and $(2t+1, t^2-t+1) = (2t+1, 7)$. Since $2t+1$ divides $(t^2-t+1)(t^2+1)/2$ and t^2+1 is prime to t^2-t+1, we conclude that $2t+1$ divides $5 \cdot 7$. Thus $2t+1 = 5, 7$ or 35, and $t = 2, 3$ or 17. As $t+1$ is a power of 2. We have $t = 3$.

However, in this case, we have $|G| = (t^2+1)(t^3+1) = 2^3 \cdot 5 \cdot 7$, N is an elementary abelian group of order 8, and $|C_G(a)| = |G|/(2t+1) = 2^3 \cdot 5$ for every $1 \neq a \in N$. If $C_G(N) = N$, then G/N is a subgroup of $GL_3(2)$, which is a $5'$-group, a contradiction. Thus $C_G(N)$ properly contains N, and hence $C_G(N) = C_G(a)$ for $1 \neq a \in N$. But this implies that $C_G(N)$ is the direct product of N with a group of order 5. In particular, $1 \neq O_5(C_G(N)) \leq O_5(G)$. As 5 is a divisor of $t^2+1 = 10$, this contradicts Step 1(4). $\square$

Step 3. If there is a nonabelian minimal normal subgroup N of G, then N is isomorphic to the Suzuki simple group $Sz(q)$ for some $q = 2^{2e+1} \geq 8$. Furthermore, N is the unique minimal nonabelian normal subgroup of G.

Proof. Let N be a nonabelian minimal normal subgroup. As G is a $3'$-group by Step 1(1), $N = S_1 \times \cdots \times S_m$, where $S_i \cong Sz(q)$ $(i = 1, \ldots, m)$ for some $q = 2^{2e+1} \geq 8$ from Theorem 8(1). Note that G acts transitively on $\{S_i \mid i = 1, \ldots, m\}$ by conjugation. Moreover, t is odd.

Let a be an involution of S_1. As $Sz(q)$ has one class of involutions of length $(q-1)(q^2+1)$, we see that a^G is the disjoint union of the sets of involutions of S_i for $i = 1, \ldots, m$. In particular, $|a^G| = m(q-1)(q^2+1)$. Note that $a^G \cap \Delta^c \neq \emptyset$, for otherwise t^2 would be at most $t^2 - t$ by Lemma 10(2). Thus it follows from Lemma 6(1)(2) that

$$|a^G| = m(q-1)(q^2+1) \geq t+1.$$

On the other hand, as a Sylow 2-subgroup of N is of order $(q^2)^m$ and $|G|_2 = 2(t+1)_2$, we have

$$q^{2m} \leq 2(t+1).$$

From those two inequalities, we have

$$q^{2m} \leq 2(t+1) \leq 2m(q-1)(q^2+1) < 2mq^3.$$

Now suppose $m \geq 2$. Then we have $q^{2m-3} < 2m$ from the above inequality, where $2m - 3 \geq 1$. However, then we have

$$2m > q^{2m-3} \geq (1+7)^{2m-3} \geq 1 + 7(2m-3),$$

or equivalently, $5 > 3m$, which is impossible for $m \geq 2$. Thus $m = 1$ and $N \cong Sz(q)$.

Now let M be a minimal normal subgroup of G which is nonabelian and distinct from N. Then $M \cong Sz(q')$ for some $q' = 2^{2e'+1} \geq 8$ by the first part of the claim. Replacing M by N if necessary, we may assume that $q \leq q'$. As N is normal in G and N has a single class of involutions, we have $a^G = a^N$ for an involution a of N. Then $|a^G| = (q-1)(q^2+1)$, which is at least $t+1$ as we saw above. Thus

$$q^3 > (q-1)(q^2+1) \geq t+1.$$

On the other hand, $M \times N$ has a Sylow 2-subgroup of order $q^2(q')^2$, and so

$$q^4 \leq q^2(q')^2 \leq |G|_2 \leq 2(t+1).$$

From those two inequalities, we have

$$q^4 \leq 2(t+1) < 2q^3,$$

or equivalently $q < 2$, which is impossible. □

Step 4. Assume that t is odd. For a central involution a of G (i.e., $C_G(a)$ contains a Sylow 2-subgroup of G), the order of a Sylow p-subgroup of $C_G(a)$ is at most $t-1$ for every prime p dividing $t^2 - t + 1$.

Proof. We have

$$|a^G \cap \Delta||C_G(a)| = (t^2+1)|\mathcal{L}_1(a)| = (t+1)(t^2+1+tu_a)$$

for some integer u_a, applying Lemma 2(1) and Lemma 3. As $(t^2+1, t+1) = 2$ and $(t^2+1, t) = 1$, this implies that $u_a = ((t^2+1)/2)v_a$ for some integer v_a, and

$$(t^2+1)|\mathcal{L}_1(a)| = (t+1)\left(\frac{t^2+1}{2}\right)(2+tv_a).$$

As a is central, $(t^2+1)|\mathcal{L}_1(a)| = |a^G \cap \Delta||C_G(a)|$ is divisible by $2(t+1)_2 = |G|_2$. Hence $2+tv_a$ is even, which implies that v_a is even, as t is odd. Thus writing $v_a = 2w_a$ for an integer w_a, we have

$$|\mathcal{L}_1(a)| = (t+1)(1+tw_a).$$

As the left hand side of this equation is nonnegative, we have $w_a \geq 0$. Then we calculate

$$|a^G \cap \Delta^c||C_G(a)| = |G| - |a^G \cap \Delta||C_G(a)| = 2(t+1)\frac{(t^2+1)}{2}t(t-w_a-1).$$

Now for every prime p dividing t^2-t+1, the p-part of $|C_G(a)|$ is prime to t, $t+1$ and t^2+1 by Step 1(2); the above equality implies that $|C_G(a)|_p$ divides $t-w_a-1$ and, in particular,

$$|C_G(a)|_p \leq t-1-w_a \leq t-1,$$

as we claimed. $\square$

Step 5. There is no nonabelian normal subgroup of G.

Proof. Suppose G has a nonabelian normal subgroup, and let N be a minimal one. Then $N \cong Sz(q)$ for some $q = 2^{2e+1}$ by Step 3. The group N is contained in $E(G)$, the group generated by all quasisimple subnormal subgroups of G. In particular, $E(G) \neq 1$.

As G is a $3'$-group, each quasisimple subgroup L of $E(G)$ is a central extension of the simple Suzuki group $Sz(q)$. Hence L is simple, as the Schur multiplier of $Sz(q)$ is trivial. Then $E(G)$ is a direct product of nonabelian simple groups. From the latter part of Step 3, we have $N = E(G)$.

Assume that a normal subgroup $C_G(N)$ of G is not trivial. Then the generalized Fitting subgroup $F^*(C_G(N)) = E(C_G(N))F(C_G(N))$ of $C_G(N)$ is nontrivial, as in general $F^*(H) \neq 1$ whenever a finite group H is nontrivial by the fundamental property $C_H(F^*(H)) \leq F^*(H)$ of the generalized Fitting subgroup. Since $E(C_G(N)) \leq E(G) = N$, we have $E(C_G(N)) = 1$. Thus $F^*(C_G(N)) = F(C_G(N)) \neq 1$. It follows from Step 1(3)(4) and Step 2 that $F(C_G(N))$ (which is normal in G) is a direct product of some p-subgroups for primes p dividing t^2-t+1. Take such a prime p for which $M := O_p(C_G(N)) \neq 1$. Then $|M| \geq t+2$ by Step 1(3).

Note that N contains a central involution a of G, as $P \cap N$ is a nontrivial normal 2-subgroup of P for each Sylow 2-subgroup P of G. However, this contradicts Step 4, as $M \leq C_G(N) \leq C_G(a)$ and M is a p-group of order at least $t+2$ and p divides t^2-t+1.

Thus $C_G(N) = 1$. Then G/N is a subgroup of the outer automorphism group of $N \cong Sz(q)$, which is a cyclic group of order $2e+1$. Thus $|G|$ is a divisor of $|N|(2e+1) = q^2(q-1)(2e+1)(q^2+1)$. In particular,

$$|G| \leq q^2(q-1)^2(q^2+1) < q^6,$$

as $q - 1 = 2^{2e+1} - 1 = (1+1)^{2e+1} - 1 > (2e+1)$.

Now q^2 is a divisor of $|G|_2 = 2(t+1)_2$ (note that t is odd). Assume that $t+1$ is a power of 2 and $q^2 = 2(t+1)$. Then $q^2 + 1 = 2t + 3$ divides $|N|$ and so $|G| = (t+1)(t^2+1)(t^2-t+1)$. As $(2t+3, t+1) = 1$, $(2t+3, t^2+1) = (2t+3, 3t-2) = (2t+3, 13)$ and $(t^2-t+1, 2t+3) = (2t+3, 5t-2) = (2t+3, 19)$, the common divisor of $2t+3$ and $|G|$ divides $13 \cdot 19$. Thus $2t+3 = 13$, 19 or 247, and $t = 5, 8$, or 122. But none of them satisfy that $t+1$ is a power of 2.

Thus q^2 is a proper divisor of $2(t+1)$, and hence $q^2 \le t+1$. Then the above inequality $|G| < q^6$ implies that

$$(t+1)(t^2+1)(t^2-t+1) < (t+1)^3,$$

and hence $t^3 + 1 < t^2 + 2t + 1$, which is impossible. This final contradiction eliminates the existence of $N \cong Sz(q)$, and the claim follows. □

Step 6. There exists a unique prime p dividing $t^2 - t + 1$ with $F^*(G) = F(G) = O_p(G) \neq 1$.

Proof. Suppose $E(G) \neq 1$. Then $E(G)$ is a direct product of the Suzuki groups by the same arguments as in the previous step, which contradicts Step 5. Thus $E(G) = 1$. Then $F^*(G) = E(G)F(G) = F(G) \neq 1$. It follows from Step 1(3)(4) and Step 2 that $F(G)$ is a direct product of $O_p(G)$ for primes dividing $t^2 - t + 1$. If $O_p(G) \neq 1$ and $O_r(G) \neq 1$ for two distinct primes p, r dividing $t^2 - t + 1$, then $|O_p(G)||O_r(G)|$ divides $t^2 - t + 1$ by Step 1(2). However, as $|O_p(G)|$ and $|O_r(G)|$ are at least $t+2$ by Step 1(3), we have $(t+2)^2 \le t^2 - t + 1$, which is impossible for a positive integer t. Thus there is a unique prime p dividing $t^2 - t + 1$ such that $F^*(G) = F(G) = O_p(G) \neq 1$. □

Now we recall the following key result on the generalized quadrangle of order (t^2, t) [6, 1.2.4]: for every triple of mutually nonconcurrent lines, there are exactly $t+1$ lines which are concurrent with all those three lines.

Step 7. For every odd prime r dividing $t^2 + 1$ and every nontrivial r-subgroup R, there are just two lines stabilized by R.

Proof. Note that $(r, t+1) = (r, t^2 - t + 1) = 1$ by Step 1(2). Thus $|R|$ divides $t^2 + 1$. As $t^2 \equiv -1 \pmod{|R|}$, we have

$$|\mathcal{L}| = (t+1)^2(t^2-t+1) \equiv (-1+2t+1)(-1-t+1) = -2t^2 \equiv 2 \pmod{|R|}.$$

Thus there are at least two lines fixed by R, as $|R| \ge r > 2$. Assume that there are three distinct lines l_1, l_2 and l_3 fixed by R. By the regularity of G, they are not concurrent with each other. Hence it follows from the fundamental result above that there are exactly $t+1$ lines, say $m_0, \ldots, m_t$, which are concurrent with all l_i $(i = 1, 2, 3)$. Since R stabilizes l_i $(i = 1, 2, 3)$, R acts on the set of those $t+1$ lines. As R stabilizes the line l_1, R permutes the points $l_1 \cap m_j$ $(j = 0, \ldots, t)$ of intersections. By the regularity of G, R fixes none of those points. Hence $|R|$ divides $t+1$. However, as $(t+1, (t^2+1)/2) = 1$, we have $R = 1$, a contradiction. Hence R fixes exactly two lines. □

3.1. Final step

Now we will complete the proof of Theorem 1 as follows. Let r be any odd prime dividing t^2+1, and let R be a Sylow r-subgroup of G. As $(t^2+1, t^2-t+1) = 1$, R acts coprimely on $F(G) = O_p(G) \neq 1$ (see Step 6).

We can see that this action is fixed point free as follows. Suppose otherwise. Then there are nontrivial elements $1 \neq x \in R$ and $1 \neq y \in O_p(G)$ commuting with each other. Thus y acts on the set $\mathcal{L}_1(x)$ of lines stabilized by x. By Step 7, $\mathcal{L}_1(x)$ consists of just two lines, and hence a nontrivial element y of odd order stabilizes both of those lines. However, then y acts on the set of t^2+1 points on each of those lines, and hence its order $o(y)$ is a proper power of p dividing t^2+1. This contradicts the fact that $(t^2+1, t^2-t+1) = 1$.

In particular, $|O_p(G)| - 1$ is divisible by $|R| = (t^2+1)_r$ for every odd prime divisor r of t^2+1. Now $(t^2+1)_2 =: \varepsilon = 1$ or 2, according to whether t is even or odd. Then we conclude that

$$|O_p(G)| - 1 = \alpha(t^2+1)/\varepsilon$$

for some positive integer α. On the other hand, as $|O_p(G)|$ divides t^2-t+1 by Step 6, there is a positive integer β with

$$t^2 - t + 1 = \beta|O_p(G)| = \beta\left(\alpha\frac{(t^2+1)}{\varepsilon} + 1\right).$$

If $\beta \geq 2$, then $t^2 - t + 1 \geq 2(\alpha((t^2+1)/\varepsilon) + 1) \geq t^2 + 1 + 2$, which is impossible. Thus $\beta = 1$ and $t^2 - t = \alpha((t^2+1)/\varepsilon)$. However, as $(t^2+1)/\varepsilon$ is prime to both t and $t-1$, this is also impossible.

References

[1] S. De Winter, K. Thas, Generalized quadrangles with an abelian Singer group, 2004 (preprint).
[2] D. Ghinelli, Regular groups on generalized quadrangles and nonabelian difference sets with multiplier −1, Geom. Dedicata 41 (1992) 165–174.
[3] D.M. Goldschmidt, 2-fusion in finite groups, Ann. of Math. 99 (1974) 70–117.
[4] G. Glauberman, Factorization in local subgroups of finite groups, in: CBMS, vol. 33, Amer. Math. Soc., Providence, 1977.
[5] U. Ott, Some remarks on representation theory in finite geometries, in: Geometries and Groups, in: Lecture Notes in Math., vol. 893, 1981, pp. 68–110.
[6] S.E. Payne, J. Thas, Finite Generalized Quadrangles, Pitman, Boston, 1984.